IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

ROBERT FERNANDEZ, as an individual and on behalf of all others similarly situated, Plaintiff, v. 90 DEGREE BENEFITS, LLC and 90 DEGREE BENEFITS – WISCONSIN (f/k/a EBSO, Inc.), Defendants.	CASE NO.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Robert Fernandez ("Plaintiff") brings this Class Action Complaint as an individual and on behalf of all other individuals who are similarly situated ("Class") against Defendants 90 Degree Benefits, LLC and 90 Degree Benefits - Wisconsin, f/k/a EBSO, Inc. (collectively "90 Degree Benefits" or "Defendants"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. 90 Degree Benefits, LLC (and its wholly owned regional office, 90 Degree Benefits – Wisconsin) is a health benefits company that designs health plans and administers benefits that meet employers' health and operational needs.[1]

2. On or about June 9, 2022, 90 Degree Benefits' Wisconsin location began notifying customers and state Attorneys General about a data breach that occurred on or about February 27, 2022 (the "Data Breach").[2] Hackers obtained information from 90 Degree Benefits Wisconsin

[1] https://www.90degreebenefits.com/about.php (last visited July 11, 2022).

[2] *See, e.g.,* https://oag.ca.gov/ecrime/databreach/reports/sb24-554203 (last visited July 11, 2022).

including the personally identifiable information ("PII")[3] of thousands of individuals (including Plaintiff), including, but not limited to, their names, dates of birth, Social Security numbers, phone numbers, addresses, and health information.[4]

3. Defendant 90 Degree Benefits, on its website, promises its customers (like Plaintiff and other individuals who are similarly situated) that it "recognize[s] and respect[s] your desire for privacy when it comes to your personal and health care affairs. We attempt to protect online information according to established company security standards and practices, and we continually evaluate new technologies for safeguarding information. protects personal information" and that they "do not plan to disclose [personal information] without your consent. We maintain this information, as well as all web based transactions, according to our usual high, government regulated, security and confidentiality standards."[5]

4. Not only did hackers steal the PII of Plaintiff and Class members from Defendants, but, upon information and belief, criminals have already used the PII to attempt to steal certain of Plaintiff's and Class members' identities. Hackers accessed and then either used or offered for sale the unencrypted, unredacted, stolen PII to criminals. This stolen PII has great value to hackers.

5. Because of Defendants' Data Breach, Plaintiff's and Class members' PII is still available and may be for sale on the dark web for criminals to access and abuse for years into the future. Impacted consumers now face a lifetime risk of identity theft.

6. Plaintiff's and Class members' PII was compromised due to Defendants' negligent and/or careless acts and omissions and their failure to adequately protect the PII.

7. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect consumers' and employees' PII, (ii) warn

---

[3] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies a specific individual.

[4] https://www.90degreebenefits.com/docs/90%20Degree%20Benefits%20-%20Substitute%20Notice.pdf (last visited July 11, 2022).

[5] https://www.90degreebenefits.com/privacy.php (last visited July 11, 2022).

its customers, potential customers, employees and other consumers of their inadequate information security practices, and (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

8. Plaintiff and Class members have suffered injury as a result of Defendants' conduct. These injuries include, but are not limited to: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; and (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) deprivation of rights they possess under state consumer protection statutes.

PARTIES

9. Plaintiff Robert Fernandez is a citizen of Arizona residing in Yuma, Arizona. On or after June 9, 2022, he received a Notice of Data Breach Letter from Defendants, attached as Exhibit A.

10. Defendant 90 Degree Benefits Wisconsin, formerly known as EBSO, Inc., that has its principal place of business at 7020 N. Port Washington Road, Suite 206, Milwaukee, Wisconsin, 53217-3800. Upon information and belief, in or about December 2018, EBSO, Inc. merged with 90 Degree Benefits, LLC. 90 Degree Benefits Wisconsin is a regional office of 90 Degree Benefits, LLC.

11. Defendant 90 Degree Benefits, LLC is an Alabama limited liability company with its principal place of business at 450 Riverchase Parkway, East Birmingham, Alabama 35244. 90 Degree Benefits, LLC offers information technology services and according to its website has 24 offices serving 525,000 members nationwide.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one member of the class is a citizen of a state different from Defendants.

13. This Court has personal jurisdiction over Defendants because Defendant 90 Degree Benefits - Wisconsin (and its predecessor corporation, EBSO, Inc.) has its principal place of business within this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant 90 Degree Benefits - Wisconsin resides within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

15. Defendant 90 Degree Benefit, LLC is a provider of health plan benefit design, implementation, and operation for insurance companies and agents.[6]

16. Defendant 90 Degree Benefit through its 24 offices serves 525,000 members nationwide.[7]

17. Defendant 90 Degree Benefits Wisconsin is one of Defendant 90 Degree Benefits' regional offices. 90 Degree Benefits Wisconsin "manages all aspects of employee benefits programs for more than 100,000 plan members" and is "one of the most respected and trusted Third Party Administrators in the nation."[8]

18. 90 Degree Benefits acquired EBSO, Inc. (now called 90 Degree Benefits Wisconsin) in or about 2018.

19. There is a unity of identity between the Defendants because Defendant 90 Degree Benefits Wisconsin is a regional office of 90 Degree Benefits, LLC.

---

6 https://www.90degreebenefits.com/docs/publication-library/90%20Degree%20Difference%20Flyer.pdf (last visited July 11, 2022)

7 https://www.90degreebenefits.com/about.php (last visited July 11, 2022).

8 https://www.90degreebenefits.com/minnesota-wisconsin.php (last visited July 11, 2022)

20. In the ordinary course of doing business with Defendants, Defendants collect sensitive PII from consumers such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender;
- Health information; and
- Username and password.

21. In the course of collecting PII from consumers, including Plaintiff, Defendants promise to provide confidentiality and security for personal information, including by promulgating and placing privacy policies on their website.[9]

22. Defendant 90 Degree Benefits promises that it will protect consumers' privacy and remain in compliance with statutory privacy requirements. For example, Defendant 90 Degree Benefits states on its website "90 Degree Benefits respects your privacy and is committed to protecting it."[10]

23. Additionally, Defendant 90 Degree Benefits represented on its website "stop worrying about compliance and start letting the experts at 90 Degree Benefits help keep you on the right path."[11]

24. Defendant 90 Degree Benefit states in its Privacy Statement "we do not plan to disclose it without your consent. We maintain this information, as well as all web based

---

9 https://www.90degreebenefits.com/privacy.php (last visited July 11, 2022).

10 *Id.* (last visited July 11, 2022).

11 https://www.90degreebenefits.com/docs/publication-library/Compliance%20Services%20Flyer.pdf (last visited July 11, 2022).

transactions, according to our usual high, government regulated, security and confidentiality standards."[12]

25. Defendant 90 Degree Benefits acknowledges that it is "required by law to maintain the privacy of your verbal, electronic, or written protected health information" and "will not use or disclose your protected health information for marketing, or fundraising, and will not sell your protected health information, unless you give us a written authorization."[13]

26. Defendants, however, failed to protect and safeguard Plaintiff's and Class members PII. In fact, in their Notice Letter, there is no indication that any of the stolen PII was encrypted or redacted, including usernames and passwords.

The Data Breach

27. On or about June 9, 2022, Defendant 90 Degree Benefits Wisconsin began notifying consumers and state Attorneys General about a data breach that occurred on February 27, 2022.

28. According to its notice letters, 90 Degree Benefits Wisconsin "launched an investigation with the assistance of a leading independent digital forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization."[14]

29. The Notice of Data Breach letters claim that "systems and files containing personal information were accessed without authorization."[15]

30. However, despite first learning of the Data Breach in February 2022, Defendants did not take any "measures" to notify affected Class Members for over four months, on or about

---

[12] https://www.90degreebenefits.com/privacy.php (last visited July 11, 2022).

[13] https://www.90degreebenefits.com/docs/90DegreeBenefits_PRIVACY_NOTICE.pdf (last visited July 11, 2022).

[14] https://www.90degreebenefits.com/docs/90%20Degree%20Benefits%20-%20Substitute%20Notice.pdf (last accessed July 11, 2022).

[15] https://oag.ca.gov/system/files/ITC%20-%20Model%20Notification%20to%20Insureds%20%28Updated%29_1_1.pdf (last visited July 11, 2022).

June 9, 2022.

31. According to the data breach report that Defendants filed with The Department of Health and Human Services Office of Civil Rights, the PII of approximately 172,450 individuals was accessed by unauthorized cybercriminals in the Data Breach.[16]

Defendants Were Aware of the Risks of a Data Breach

32. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class members provided their PII to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

34. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the information technology sector preceding the date of the breach.

35. Data breaches, including those perpetrated against the information technology sector of the economy, have become widespread. For example, the United States saw 1,244 data breaches in 2018 and had 446.5 million exposed records.[17] Defendants understand this reality because 90 Degree Benefits' website states:

> Fraud is a major concern in the health care industry. It results in a loss of billions of dollars each year, and stress to consumers who are affected by it. 90 Degree Benefits is working to eliminate all instances of fraud that impact our customers, whether it is health care fraud, such as filing false claims, or electronic fraud, such as fake emails and web sites. Your help is needed in this effort. By reviewing the information provided and reporting any instances of suspected fraud, we can work together to ensure the security of our customers'

---

16 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 11, 2022). However, this information is somewhat different from the information provided to the Attorney General of Maine, which states that the Private Information of 163,483 was affected, available at https://apps.web.maine.gov/online/aeviewer/ME/40/4b4619a6-6c3a-4b4e-b723-3ba32c2f18aa.shtml (last visited July 11, 2022).

17 https://www.varonis.com/blog/data-breach-statistics (last visited July 11, 2022).

information and control the rise of health care costs. [18]

36. Indeed, data breaches, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

37. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[19] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[20]

38. The PII of Plaintiff and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of the Plaintiff and members of the Classes, including Social Security numbers, health information, and other demographic information, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and members of the Class(es) a result of a breach.

40. Plaintiff and members of the Class(es) now face years of constant surveillance of

---

[18] https://www.90degreebenefits.com/fraud.php (last visited July 11, 2022).

[19] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited July 11, 2022).

[20] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

their financial and personal records, monitoring, and loss of rights. The Class(es) are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

41. The injuries to Plaintiff and members of the Classes were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and members of the Class(es).

Defendants Fail to Comply with FTC Guidelines

42. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

43. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

44. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

45. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. Defendants failed to properly implement basic data security practices, including encryption and redaction of the stolen PII, and their failure to employ other reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes, among other things, an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

47. Defendants were at all times fully aware of their obligation to protect the PII of customers, prospective customers and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

48. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

49. Best cybersecurity practices that are standard in the information technology services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

50. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

51. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby

opening the door to the Cyber-Attack and causing the Data Breach.

The Value of PII to Cyber Criminals

52. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers; however, information such as dates of birth and Social Security numbers are even more attractive to hackers. These forms of PII are not easily changed or destroyed and can be easily used to perpetrate identity theft and other types of fraud.

53. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[21]

54. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

55. It is difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social

---

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited July 11, 2022).

[22] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 11, 2022).

Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

56. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

57. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[24]

58. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and members of the Classes stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Classes. Stolen personal data of the Plaintiff and members of the Classes represents essentially one-stop shopping for identity thieves.

---

[23] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 11, 2022).

[24] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 11, 2022).

59. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

60. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

61. Companies recognize that PII is a valuable asset, and PII is even considered a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiff and members of the Classes has a high value on both legitimate and black markets.

62. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

63. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendants' former and current customers and employees whose Social Security numbers have been compromised now face a real and imminent substantial

---

[25] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited July 11, 2022).

risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

64. The information lost in Defendants' Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, retail victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — *i.e.,* names, dates of birth, Social Security numbers, phone numbers, addresses, and health information.

65. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

66. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

Plaintiff's Experience

Plaintiff Robert Fernandez

67. Plaintiff Robert Fernandez is and during all times relevant to this complaint, a resident of Yuma (Yuma County), Arizona.

68. Soon after June 9, 2022, Plaintiff received the Notice of Data Breach from Defendant 90 Degree Benefits Wisconsin, dated on that date. *See* Plaintiff's Notice Letter, attached as Exhibit A.

69. The Notice Letter informed him that Defendant 90 Degree Benefits Wisconsin experienced a data security incident that impacted certain systems and files containing personal information.

70. According to the information provided in Defendants' website notice, the systems

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 11, 2022).

and files that were accessed without authorization "varied but potentially may have included things such as names, dates of birth, Social Security numbers, phone numbers, addresses, and health information."[27] However, on Plaintiff's Notice Letter (Exh. A), Defendants only informed Plaintiff that his "personal information" was included. This vague description gives Plaintiff Fernandez virtually no substantive information about the Data Breach. Defendants do, however, consider his risk great enough to require identity theft services.

71. As a result of the Data Breach, Plaintiff Fernandez has made efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by 90 Degree Benefits Wisconsin.

72. Plaintiff Fernandez and/or his wife now reviews his credit monitoring reports and/or checking account statements on a daily basis for fraud and other irregularities, in total spending approximately an hour a week. This is valuable time Plaintiff Fernandez and/or his wife otherwise would have spent on other activities, including but not limited to work and/or recreation.

73. Plaintiff Fernandez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

74. Plaintiff Fernandez suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that 90 Degree Benefits Wisconsin obtained from Plaintiff Fernandez; (b) violation of his privacy rights; and (c) and being at risk of imminent and impending injury arising from identity theft and fraud.

75. Moreover, subsequent to the Data Breach, Plaintiff Fernandez also experienced a significant increase in the amount of suspicious, unsolicited spam telephone calls. Each day, Plaintiff Fernandez receives approximately four scam phone calls, each of which appear to be

[27] https://www.90degreebenefits.com/docs/90%20Degree%20Benefits%20-%20Substitute%20Notice.pdf (last accessed July 11, 2022).

placed with the intent to obtain personal information to commit identity theft.

76. Plaintiff Fernandez has spent a significant amount of time since the Data Breach responding to the impacts of the Data Breach. The time spent dealing with the fallout from the Data Breach is time Plaintiff Fernandez otherwise would have spent on other activities, such as work and/or recreation.

77. As a result of the Data Breach, Plaintiff Fernandez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Fernandez will continue to be at increased risk of identity theft and fraud for years to come.

78. Plaintiff Fernandez has become anxious, nervous, and worried about this theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

79. Mr. Fernandez is aware that cybercriminals often sell Private Information, and that his could be abused months or even years after Defendants' Data Breach.

80. Upon information and belief, Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach. Plaintiff Fernandez was damaged in that his Private Information is in the hands of cyber criminals.

Plaintiff's and Class Members' Damages

81. To date, Defendants have done virtually nothing to provide Plaintiff and Class members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, reimbursements for costs and lost time Plaintiff and Class members incurred because of the Data Breach.

82. Defendants have only offered just 12 months of identity theft services through IDX, a data breach and recovery services firm,[28] only allowing 3 months for enrollment despite Defendants' even longer delay in notifying Plaintiff and the Class. This one-year limitation is

[28] *See* Notice Letter, attached as Exhibit A

inadequate when victims are likely to face many years of identity theft.

83. Defendants' offer is wholly inadequate as it fails to sufficiently compensate all victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's and Class members' Private Information.

84. Moreover, it is unclear whether credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach.

85. Furthermore, Defendants' credit monitoring offer and advice (*see* Exh. A) to Plaintiff and Class members squarely places the burden on Plaintiff and Class members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

86. Plaintiff and Class members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

88. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been forced to expend time dealing with the effects of the Data Breach.

89. Plaintiff and Class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

90. Plaintiff and Class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to more effectively target such schemes to Plaintiff and Class members.

91. Plaintiff and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

92. Plaintiff and Class members suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

93. Plaintiff and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

94. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Addressing their inability to withdraw funds linked to compromised accounts;
e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
f. Placing "freezes" and "alerts" with credit reporting agencies;
g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
h. Contacting financial institutions and closing or modifying financial accounts; and
i. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

95. Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further

breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

96. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

97. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

98. Defendant's delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[29]

99. Indeed, once a Data Breach has occurred, "[o]ne thing that does matter is hearing about a Data Breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[30]

---

[29]*Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed July 11, 2022).

[30]Consumer Reports, The Ransomware Attack Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019,

100. Although their Private Information was improperly exposed in February of 2022, the affected individuals, upon information and belief and based on the experience of Plaintiff, were not notified of the Data Breach until June 9, 2022 or later depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

101. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class has been driven even higher.

CLASS ALLEGATIONS

102. Plaintiff brings this nationwide class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All natural persons residing in the United States whose PII was compromised in the Data Breach that was announced by Defendant(s) on or about June 9, 2022 (the "Nationwide Class").

103. The Arizona Subclass is defined as follows:

> All natural persons residing in Arizona whose PII was compromised in the Data Breach that was announced by Defendant(s) on or about June 9, 2022 (the "Arizona Subclass").

104. The Arizona Subclass is referred to herein as the "Statewide Subclass" and together with the Nationwide Class, are collectively referred to herein as the "Class" or "Classes."

105. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

106. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

107. **Numerosity**: The Classes are so numerous that joinder of all members is

https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed on July 11, 2022).

impracticable. Defendants have identified approximately 172,450 individuals whose PII was improperly accessed in the Data Breach, and the large majority of Class members are apparently identifiable within Defendants' records based upon the Notice Letters Defendants sent.

108. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiff and members of the Classes;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiff and members of the Classes;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiff and members of the Class secure and to prevent loss or misuse of that PII;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff and members of the Classes damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiff and members of the Classes that their PII had been compromised;

j. Whether Defendants violated common law and statutes invoked below; and

k. Whether Plaintiff and the other members of the Classes are entitled to extended credit monitoring and other monetary relief.

109. **Typicality**: Plaintiff's claims are typical of those of the other members of the

Classes because all had their PII compromised as a result of the Data Breach due to Defendants' misfeasance.

110. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

111. **Superiority and Manageability**: Under Rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

112. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to the Subclass as a whole.

113. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendants breached a legal duty to Plaintiff and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff, the Class, and the Statewide Subclass Against All Defendants)

114. Plaintiff re-alleges and incorporates by reference the above allegations.

115. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

116. The legal duties owed by Defendants to Plaintiff and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in its possession;

b. To protect PII of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

117. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the

Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

118. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiff and Class members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

119. Defendants breached their duties to Plaintiff and Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

120. Defendants knew or should have known that their security practices did not adequately safeguard Plaintiff's and the other Class members' PII.

121. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiff and the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Defendants' possession and control.

122. Defendants breached the duties they owe to Plaintiff and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

123. Due to Defendants' conduct, Plaintiff and Class members are entitled to extended credit monitoring. Credit monitoring for at least 10 years is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against the Class members.

124. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[31] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

125. As a result of Defendants' negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

[31] In the recent Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

126. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiff, the Class, and the Statewide Subclass Against All Defendants)

127. Plaintiff re-alleges and incorporates by reference the above allegations.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

129. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

130. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

131. Plaintiff and members of the Classes are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

133. As a direct and proximate result of Defendants' negligence per se, Plaintiff and members of the Classes have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Classes.

134. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM FOR RELIEF
Violation of Arizona's Consumer Fraud Act ("ACFA")
Title 44, Chapter 10. Article 7, Section 44-1521, *et seq.*
(On behalf of Plaintiff Fernandez and the Arizona Subclass)

135. Plaintiff re-alleges and incorporates by reference the above allegations.

136. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or

advertisement of any merchandise whether or not any person has in face been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

137. Plaintiff and State Subclass Members are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

138. Defendants provides "services" as that term is included in the definition of "merchandise" under Ariz. Rev. Stat. § 44-1521(5), and Defendants is engaged in the "sale" of "merchandise" as defined by Ariz. Rev. Stat. § 44-1521(7).

139. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ACFA) in violation of the ACFA, including but not limited to the following:

a. Failing to maintain sufficient security to keep Plaintiff's and Class Members' confidential medical, financial and personal data from being hacked and stolen;

b. Failing to disclose the Data Breach to Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B);

c. Misrepresenting material facts, pertaining to the sale of health benefit services by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Misrepresenting material facts, in connection with the sale of health benefit services by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PII;

e. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Class Members' PII;

f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of health benefit services by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected

in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including HIPAA and Section 5 of the FTC Act;

g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to disclose the Data Breach to Class members in a timely and accurate manner;

h. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Class members' PII from further unauthorized disclosure, release, data breaches, and theft.

140. The above unlawful, unfair, and deceptive acts and practices by Defendant 90 Degree Benefits and Defendant 90 Degree Benefits Wisconsin were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

141. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class members' PII and that risk of a data breach or theft was high. Defendant 90 Degree Benefits and Defendant 90 Degree Benefits Wisconsin's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Members of the Class.

142. As a direct and proximate result of Defendants' deceptive acts and practices, the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

143. Plaintiff and Class Members are entitled to all monetary and non-monetary relief available for Defendants' violations of the ACFA.

FOURTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiff, the Nationwide Class,
and the Statewide Subclass Against All Defendants)

144. Plaintiff re-alleges and incorporates by reference the above allegations.

145. Defendants owe duties of care to Plaintiff and Class members which require them to adequately secure their PII.

146. Defendants still possess Plaintiff's and Class members' PII.

147. Defendants do not specify in the *Notice of Data Breach* letter what steps they have taken to prevent this from occurring again.

148. Plaintiff and Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

149. Plaintiff, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Class members for a period of ten years; and

h. Meaningfully educating Plaintiff and Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment against the Defendants and that the Court grant the following:

a. An order certifying the Class and Subclass as defined herein, and appointing Plaintiff and his counsel to represent the Classes;

b. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and the members of the Class(es);

c. Injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

   i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendants to protect, including through encryption, all data

collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs

sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

e. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

f. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

g. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: July 12, 2022

Respectfully Submitted,

/s/ Lisa A. White_____
By: Lisa A. White, TN Bar # 026658
Admitted to the ED of Wisconsin

Gary E. Mason (admission pending)
Danielle L. Perry (admission pending)
Lisa A. White
MASON LLP
5101 Wisconsin Ave. NW Ste. 305
Washington DC 20016
Phone: 202.640.1160
Fax: 202.429.2294
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff and the Class